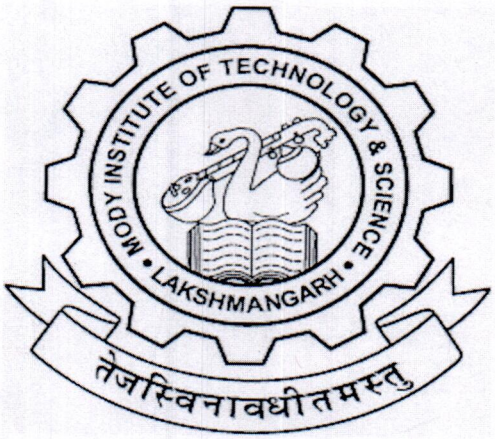
Mody Institute of Technology and Science

Lakshmangarh

Faculty of Engineering and Technology

Design and Implementation of Techniques to Resolve Interoperability Issues in Public Key Infrastructure



Research Proposal

Ph.D Candidate Name	:	Sarvesh Panwar
Enrollment Number	:	110432
Department	:	Computer Science and Engineering
Supervisor Name	:	**Prof. (Dr.) Prema K.V**

Table of Contents

Sr. No.	Topic	Page No.
1.	Introduction	1
1.1	Digital Certificates	1
1.2	PKI Components	3
1.3	Functions of PKI	4
1.4	Application of PKI	4
1.5	PKI in India	5
1.6	Goals of PKI	5
2.	Interoperability	6
2.1	Interoperability areas	6
2.2	Interoperability Challenges	9
3.	Scope of work	9
4.	Objectives	10
5.	Proposed Approach	15
6.	Research Methodology	17
7.	Time Plan	19
8.	Hardware & Software Requirements	19
9.	Conclusion	20
List of Publication		21
References		22

1. Introduction

Organizations need enhanced security for data and strong credentials for identity management. We can use certificates to secure data and manage identification credentials from users and computers both within and outside the organization. Most commonly used certificates are Digital Certificates, which are part of the public key infrastructure (PKI).

A public key infrastructure (PKI) is the combination of software, encryption technologies, processes, and services that enable an organization to secure its communications and business transactions. **The ability of a PKI to secure communications and business transactions is based on the exchange of digital certificates between authenticated users and trusted resources.**

Ever since applications entered the Internet era, the need for secure authentication has been a major issue. In early 90's asymmetric cryptography became an affordable technology for the computational power of the standard workstation and a lot of effort was devoted to support it by creating and managing public-key certificates (PKC) through public-key infrastructures (PKIs) [22].

PKI is a framework for creating a secure method for exchanging information based on public key cryptography. The foundation of a PKI is the certificate authority (CA), which issues digital certificates that authenticate the identity of organizations and individuals over a public system such as the Internet. The certificates are also used to sign messages, which ensure that messages have not been tampered with [1].

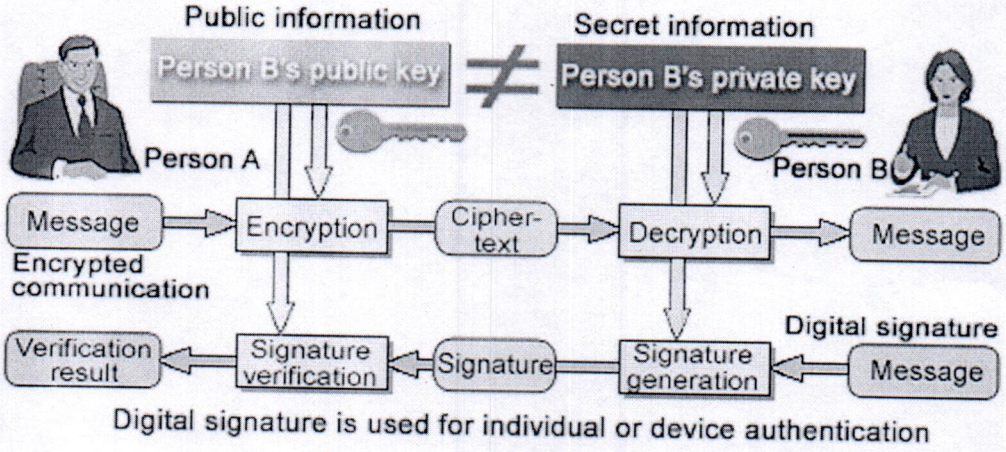


Figure 1.1: Public key cryptosystem

1.1 Digital Certificates

A digital certificate is the combination of a statement and a digital signature of the statement [18]. Digital Certificate provides a means of proving your identity in electronic transactions; just like a driver's license or a passport. You can present a Digital Certificate electronically to prove your identity or your right to access information or services online.

A Digital Certificate is issued by a Certification Authority (CA) and signed with the CA's private key. It typically contains:

- Owner's public key
- Owner's name
- Expiration date of the public
- Name of the issuer (the CA that issued the Digital Certificate)
- Serial number of the Digital Certificate
- Digital signature of the issuer

The most widely accepted format for digital certificates is defined by the CCITT X.509 international standard and the most widely used standard for digital certificates is X.509.

Electronic commerce, electronic banking, and other online transactions are becoming more common, offering the convenience and flexibility to the government and business processes. However, it brings along the concerns about privacy and security of the electronic data transacted. Encryption of the data alone is not enough, as it provides no proof of the identity of the sender of the encrypted information. Thus the digital signature technology is used which makes the use of the digital certificate, which provides an easy electronic means of verifying sender's identity ensuring the non-repudiation.

For example, a customer shopping at an electronic mall run by Netscape's server software requests the Digital Certificate of the server to authenticate the identity of the mall operator and the content provided by the merchant. Without authenticating the server, the shopper should not trust the operator or merchant with sensitive information like a credit card number. The Digital Certificate is instrumental in establishing a secure channel for communicating any sensitive information back to the mall operator.

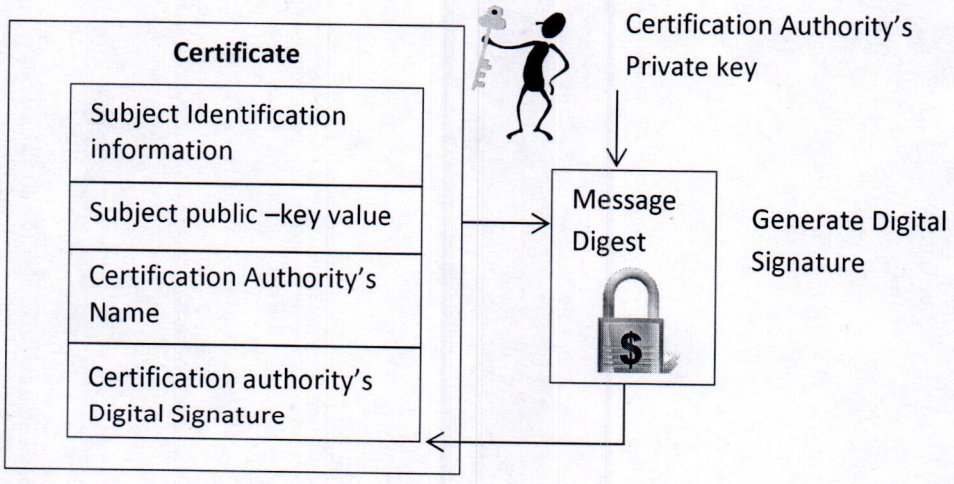


Figure 1.2 : Digital Signature for a Certificate

Certificate formats

A digital certificate is basically a collection of identifying information bound together with a public key and signed by a trusted third party to prove its authenticity. A digital certificate can be one of a number of different formats.

Two different certificate formats are:-

- PGP certificates
- X.509 certificate

1.2 PKI Components

There are four main components in PKI:

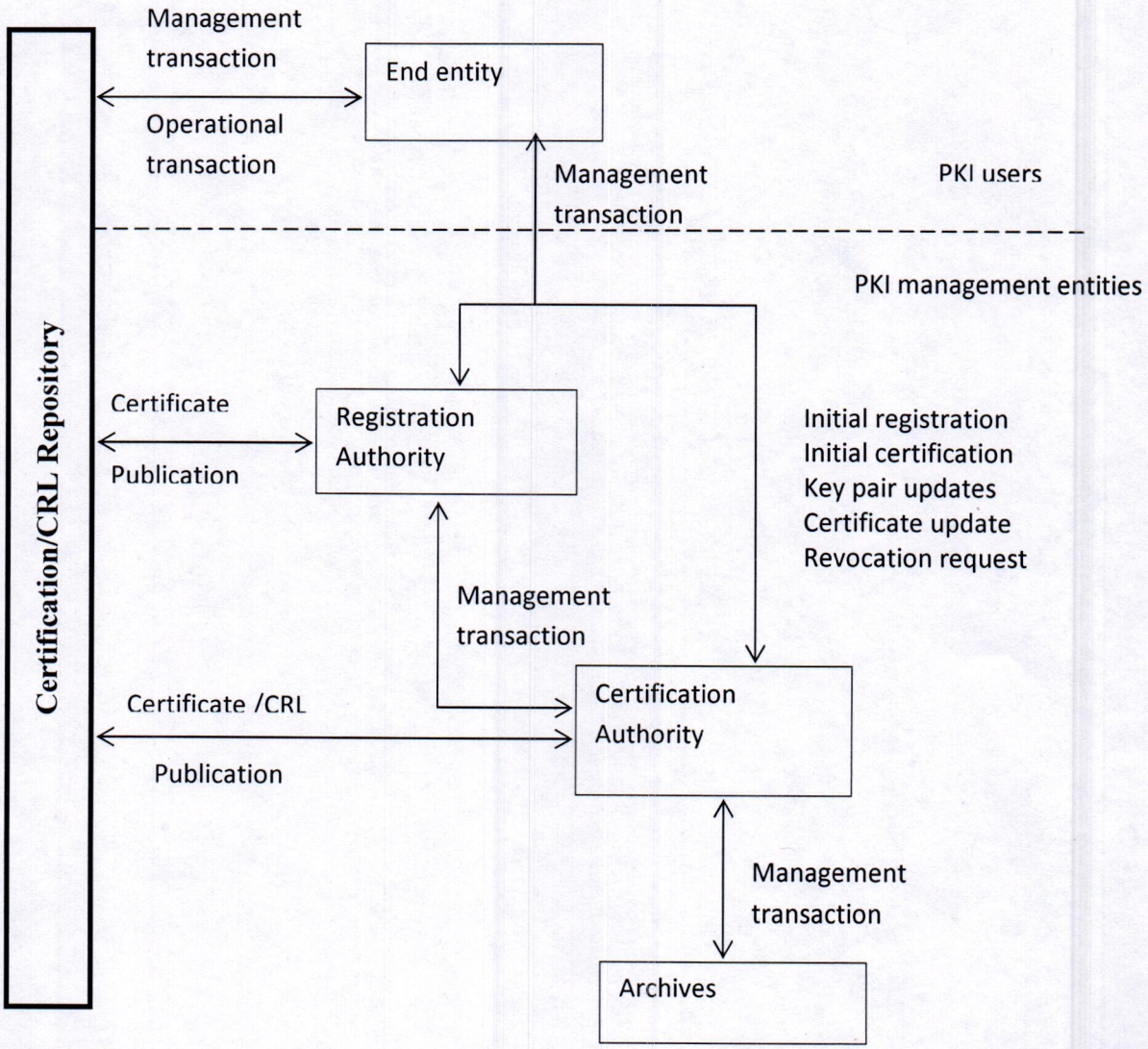


Figure 1.3 : PKI Components

- Certificate Authority (CA)
- Registration Authority (RA) for certificate content control and to make sure that it belongs to its owner.
- Repository for distribution of certificates and certificate cancellation lists with maximum efficiency and accessibility.
- Archive for the safe and long-term storage of information [4,7].

1.3 Functions of PKI [3]

- Registration
- Initialization
- Certification
- Key pair recovery
- Key generation
- Key update
- Cross-certification
- Revocation

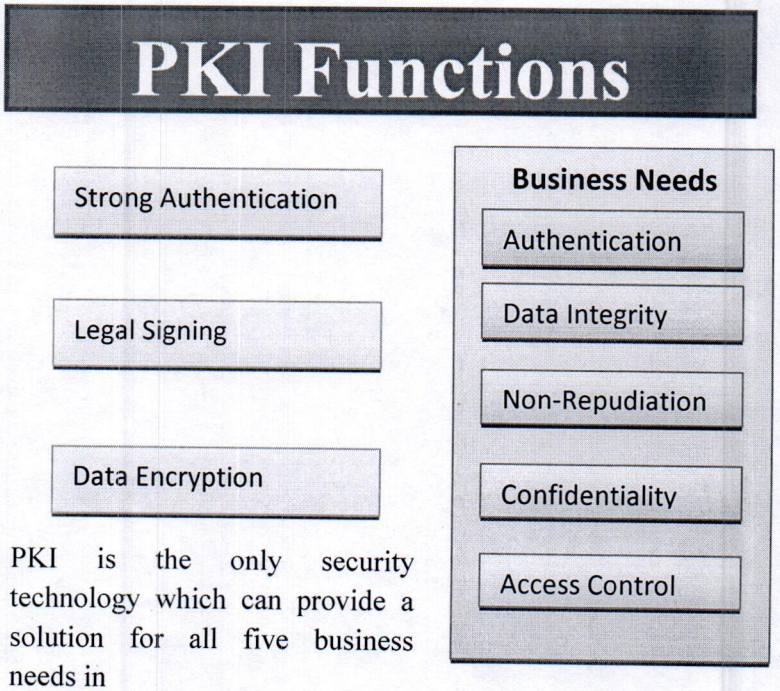


Figure 1.4 : Functions of PKI

1.4 Application of PKI

A PKI is the first step of secure electronic processing for an organization. Some typical organizations and their PKI uses are given below.

- Physical security companies (for large malls, airports, business centers): to build a common electronic platform for the physical security.
- Financial institutions: to support secure online banking and secure card transactions.
- Insurance companies: to gather their agencies and customers under a common roof for secure claim processing, renewals and payments.
- DMVs: to facilitate title and driver's license applications, renewals as well as written testing.

- State governments and government agencies: to build e-government.
- Universities/community colleges: to create a centralized identification system to be used for campus computer system logon, library checkout, on-campus businesses, security, etc.
- E-mail with customers, partners and Employees
- E-Commerce including data exchange and financial transactions.
- Digital contract including loans, leases and Mortgages.
- Remote Access to corporate databases.

1.5 PKI in India

- TCS Digital Certification.
- Implementation of Provably Secure Public Key Protocols- funded by Indian Statistical Institute- ISI, Kolkota.
- Institute for development and research in banking technology (Established by Reserve Bank of India)

1.6 Goals of PKI [6]

The central goal of Public Key Infrastructure (PKI) is to enable trust judgments between distributed users. At its core, a PKI depends on certificates: signed bindings of public keys to key holder properties. Effective use of PKI requires use of these certificates; however, effective use of certificates requires many additional services, such as OCSP servers, CRL repositories, time stamping services, etc. As a consequence, client-side PKI tools need to be able to discover and use these services; server-side PKI tools need to be able to provide these services and enable client tools to discover them [21].

These are the following issues for PKI interoperability.

- PKI profile Standards
- Development and application of Bridge Model
- Personnel education of PKI technology
- Rules of industrial forums and Merchants
- New models for establishing liability transfer
- Certificate Translation Services
- Government Support
- The relationships between Bridge CA
- PKI current situations

2. Interoperability

- Interoperability – also known as **Multi-Vendor** interoperability- where different technologies from different vendors are used by different clients including different applications.
- Interoperability helps to support transactions between different parties that use different technology supplied by the different vendors, and lowers the risk of deploying a PKI-based solution.

2.1 Interoperability Areas

The PKI interoperability framework adopted by the PKI Forum is based on a presentation offered by Tim Polk of NIST at the first PKI Forum Members Meeting in Foster City, CA, USA on 6-8 March 2000, in which he identified three major interoperability areas as follows:

A. Component-Level Interoperability;
B. Application-Level Interoperability; and
C. Inter-Domain Interoperability.

(A) Component-Level Interoperability

Component-level interoperability deals with interaction between devices directly supporting and/or consuming PKI-related services. For the sake of simplicity, we are only considering intra-domain interoperability here. Typically more complex issues are associated with inter-domain interoperability. Figure 2.1 allows for the possibility of additional CAs that, in this context, would represent intra-domain cross-certification (i.e., peer-to-peer relationships in the case of a meshed trust model or superior/subordinate relationships in the case of a hierarchy) [6][10].

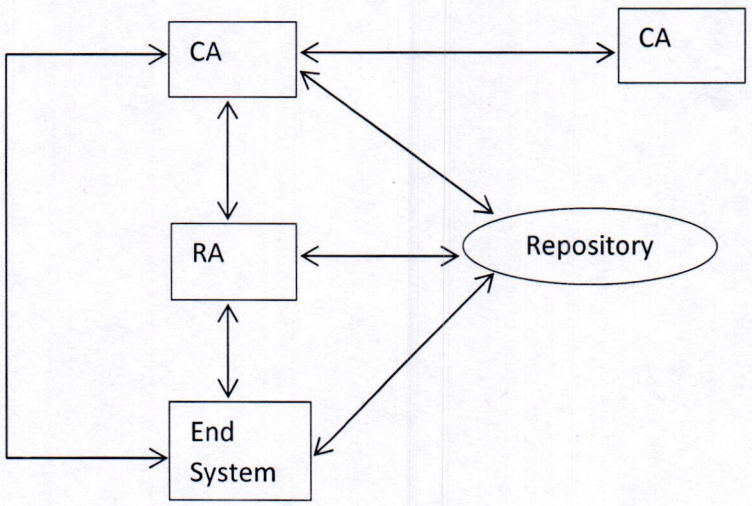


Figure 2.1: Component level interoperability

Component-level interoperability includes the following considerations:

1. Common protocols and message formats (e.g., PKIX-CMP and PKIX-CRMF) must be implemented between applicable PKI components – this applies to CA-CA, CA-RA, client-CA, and client-RA interaction;
2. Common algorithms for entity authentication and the protection of the exchanged data between PKI components must be implemented (e.g., cryptographic algorithms to support secure CMP exchanges);
3. Common protocols and underlying authentication scheme must be supported to facilitate the storage and retrieval of certificates and certificate revocation information between the repository and the PKI components;
4. Common certificate revocation mechanisms must be supported (e.g., CRLDPs, OCSP);
5. A standard cryptographic interface in support of a hardware security module at the CA must be supported; and
6. Support for flexible certificate types and profiles should be provided.

(B) Application-Level Interoperability

Application-level interoperability is concerned with compatibility between two peers, regardless of the supplier of the application or any ancillary infrastructure components used to support the application. For example, two S/MIME-based e-mail clients must be capable of interoperating with one another, even when the application software is supplied by two different vendors, the applications run on two different platforms, and each S/MIME client uses PKI technology supplied by different vendors.

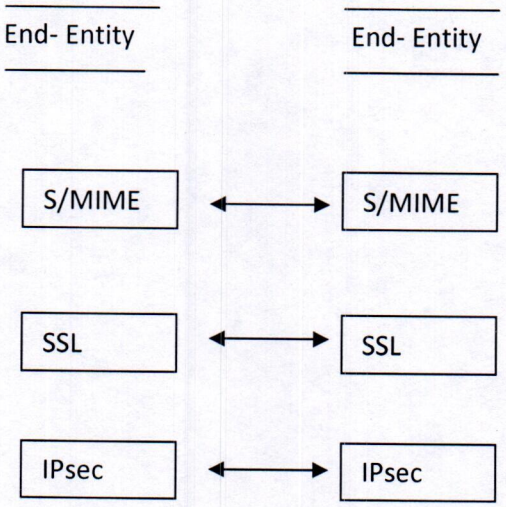


Figure 2.2 : Application Level Interoperability

For example, IPSec is considered to be an application in this context.

1. Certificate and certificate status information must be compatible (at least to the extent that any incompatibilities will not affect interoperability);
2. Business controls must be implemented to ensure that certificates that are being used are consistent with intended key usage and any associated constraints;
3. Algorithms (including cryptographic algorithms and key sizes) must be compatible;
4. Data encapsulation and encoding formats (e.g., file format, message formats, etc.) must be compatible;
5. Underlying communications protocols used to exchange information between peers must be compatible; and
6. Any in-band methods for sharing public-key related information (e.g., end-entity and CA certificates, certificate status, etc.) must be compatible. Single-key, dual-key and N-key hybrids must be supported; and
7. Private credentials must be accessible regardless of storage method (e.g., software, smart card, h/w token).

(C) Inter-Domain Interoperability

Inter-domain interoperability deals with the issues and options associated with achieving interoperability between two otherwise isolated PKI domains [5]. Inter-domain interoperability is perhaps the most complex of the three interoperability areas, since it involves, among other things, the cooperation of multiple administrative domains. It represents the requirement to exchange PKI-related information between the two PKI domains (which can be accomplished in a variety of ways) [6][16].

Inter-domain interoperability involves a number of challenges, both technology and policy-related. The following issues must also be addressed:

1. A method for establishing trust relationships between the PKI domains is required (see the PKI Forum's CA-CA Interoperability White Paper, March 2001 for a discussion of options);
2. Appropriate PKI-related information in one domain must be made available to the other, and vice versa (as applicable based on the associated trust relationship); and
3. Each PKI domain must agree to adhere to certain policies (e.g., what a given certificate is to be used for), and each PKI domain needs to have mechanisms in place to enforce adherence to the agreed-upon policies.

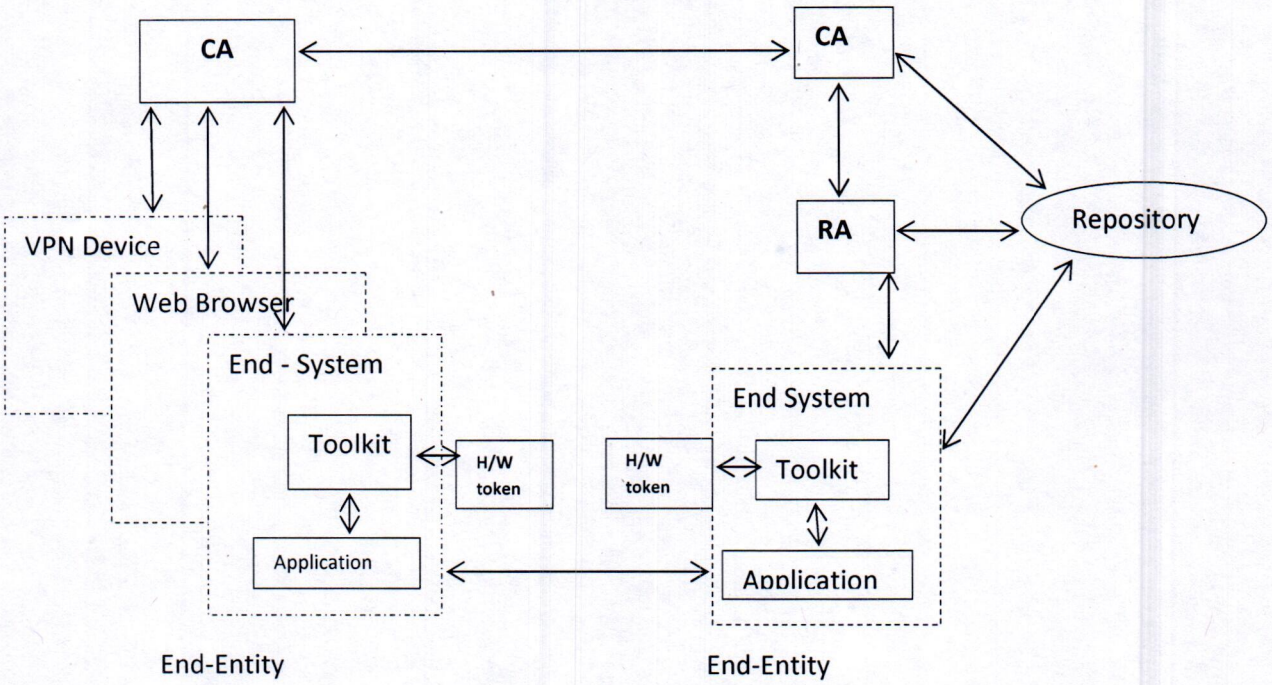


Figure 2.3 : Interoperability Boundaries

2.2 Interoperability Challenges [8][6][13]

- Different developments of X.509
- Different policies for issues certificates
- Different requirements for issuing certificates.
- Different library protection
- Different properties of PKI Applications
- Different standards for storing and retrieving certificates
- Different PKI knowledge among organization staff.

3 Scope of Work

PKI (Public Key Infrastructure) technology is an effective way to solve network security issues, PKI is an infrastructure to implement and provide security services through public key concepts and techniques [2].

The secured on line transmission of information in e-commerce is the primary objective of the public key infrastructure. It provides a means for the following:-

Authentication – Mechanisms to strongly authenticate user identities;

Confidentiality – Ability to enable strong encryption that can protect the privacy of information transferred during a transaction;

Integrity – Capability to ensure that transactions have not been modified by an unauthorized party;

Key recovery – Capability for authorized users to obtain cryptographic keys needed to recover information protected with encryption keys that may have been lost or damaged; and

Non-repudiation – Ability to validate that specific users were involved in a transaction.

However if PKIs are different then interoperability issues arise which need to be resolved. Much work has not been done in this regard and organizations usually handle this problem manually as and when it arises. Automation of the detection of interoperability mismatch and resolution is the scope of our work.

4. Objective

The interoperability problem appears when two or more heterogeneous resources are put together. One of the main problems in public key infrastructures (PKI) is currently the lack of interoperability at international level, which is greatly dependent on the automation of the cross-certification procedure using certificate policies (CP). However, cross certification is not yet technically provided in an automated way, resulting often in a difficult and time-consuming paper-based process, which reduces the flexibility and usability of the method itself. The lack of automated cross-certification is largely due to the inadequate standardization of the certificate policies (CP), which define the PKI certificates' profile and, thus, form the basic comparison criteria for the mutual acceptance of CAs [23].

In most cases, organizations need seamless application-to-application interoperability. One could argue that this is all an organization needs to worry about. However, other aspects of interoperability, including the ability to mix and match various components from one vendor with another are also important. Many corporations are processing transactions between their enterprise domain and other enterprise domains - in order to conduct B2B transactions. This is of particular concern when the technology deployed in one domain is supplied by a different vendor than the technology deployed in another. Organizations are also concerned with risk mitigation. They want assurance that they can have graceful transition to another vendor's products without having to start their deployment over from scratch [6].

Inter-Domain Interoperability

PKI interoperability is the ability to mix and match various PKI components from one vendor with those of another. Inter-domain interoperability deals with the issues and options

associated with achieving interoperability between two otherwise isolated PKI domains. Inter-domain interoperability is perhaps the most complex of the three interoperability areas, since it involves, among other things, the cooperation of multiple administrative domains. It represents the requirement to exchange PKI-related information between the two PKI domains (which can be accomplished in a variety of ways). The bi-directional arrow between the two domain boundaries can be facilitated in a number of ways, as discussed in the PKI Forum's CA-CA Interoperability White Paper, March 2001 [8][15].

Inter-domain interoperability involves a number of challenges, both technology and policy-related. The following issues must also be addressed:

1. A method for establishing trust relationships between the PKI domains is required (see the PKI Forum's CA-CA Interoperability White Paper, March 2001 for a discussion of options);
2. Appropriate PKI-related information in one domain must be made available to the other, and vice versa (as applicable based on the associated trust relationship); and
3. Each PKI domain must agree to adhere to certain policies (e.g., what a given certificate is to be used for), and each PKI domain needs to have mechanisms in place to enforce adherence to the agreed-upon policies.

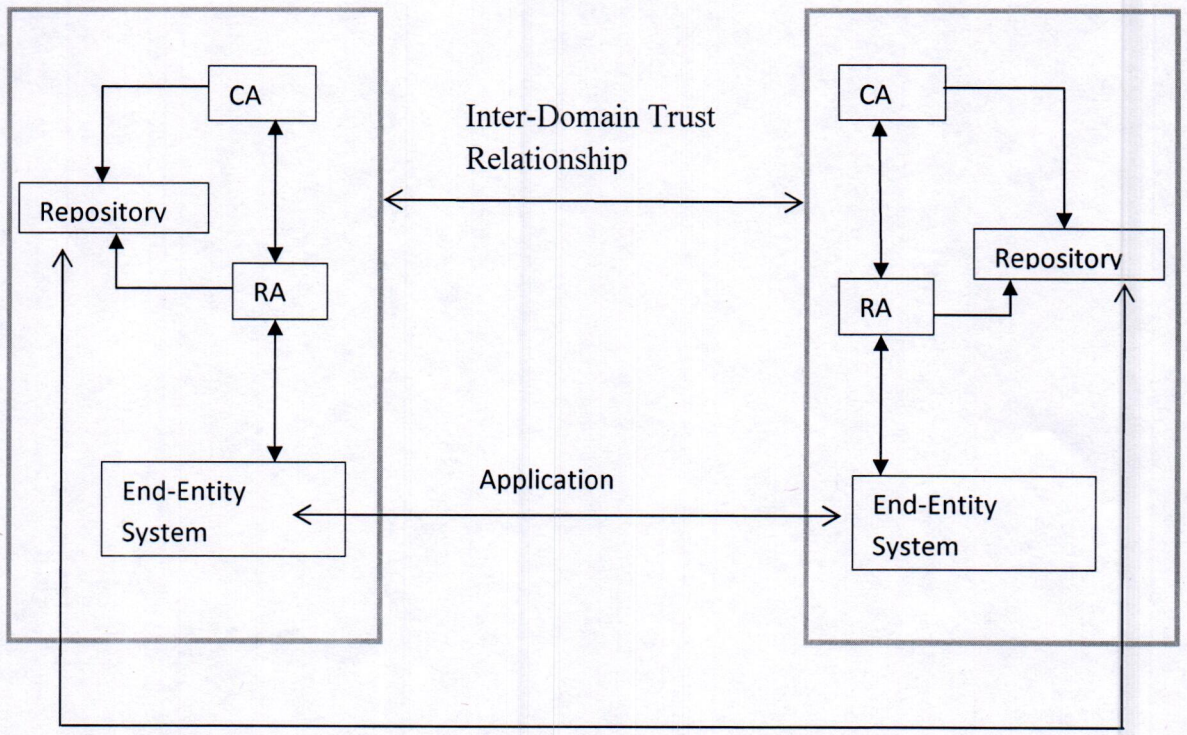


Figure 4.1: PKI Interoperability Framework[10]

The major issue arises because of the different policies adopted by different organizations. In our research work we divide the objectives into three sub parts:-

Objective 1

1. **Establishing Efficient Trust Model for PKI interoperability**
   A trust model provides a framework for building a trust relationship among end entities.
   - Peer to Peer Trust Model
   - Hierarchical Trust Model
   - Hybrid Trust Model
   - Bridge-CA

PKI Trust Models

There are some models available for definition of CA communication. Model selection affects interoperability. There are following models:-

Hierarchical Model

In a hierarchy, CAs is assembled under a common root-CA, which issues certificates to subordinate CAs. Although a hierarchy may in theory have an arbitrary number of levels, practical systems usually have two levels: root-CA and certificate issuing CAs [4]. It has a single root CA and is holding all certificates; all end-users refer to and trust it for all transaction. Hierarchical Model can also have Registration Authorities (RAs) which are the initial processing points of user's identification and issues key pairs. RA produces flexibility for smaller groups by allowing them to have their own local and customized services.

This model saves us from various interoperability problems by providing a single convenient point of access. But when number of user's increases, it is having sometimes limitation for example

- It is obvious when the number of users increase; it increases the workload for example technical and administrative point of view.
- Different users can have different requirements that could be difficult for a single CA to address these all.
- Security can also be a concern because a Single CA could be target for hackers and a security collapse could occur in the system.

Although CA model is the basic unit of all PKIs, but as discussed above interoperability could be a problem. The model can have significant result if a logical variation is introduced resulting in a **strict hierarchy model**.

Strict hierarchy model have one main CA known as trusted root CA whose job is to issue a certificate to its subordinate CAs. The subordinates can further issue certificates to their subordinates CA and so the hierarchy works. Each CA in the hierarchy is trusted because the higher certifying CA in the hierarchy is trusted. Only the root CA must be trusted on its own. The advantage of hierarchical structure is a short and definite path and is easily traceable back to a trusted source.

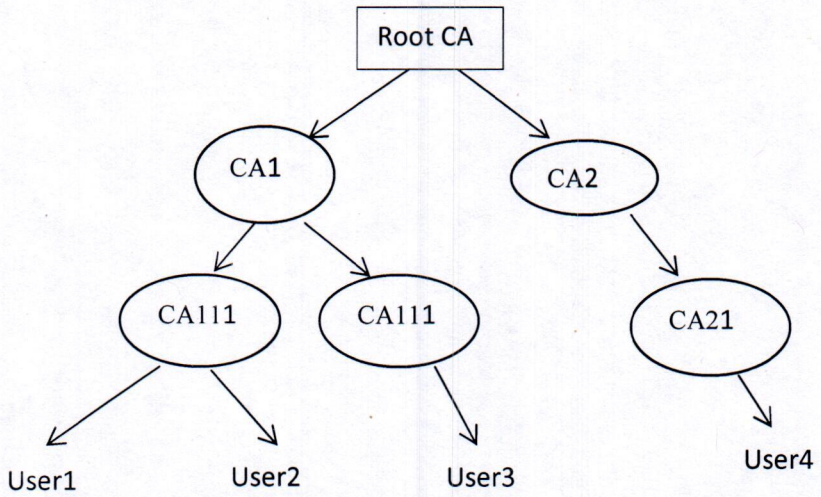
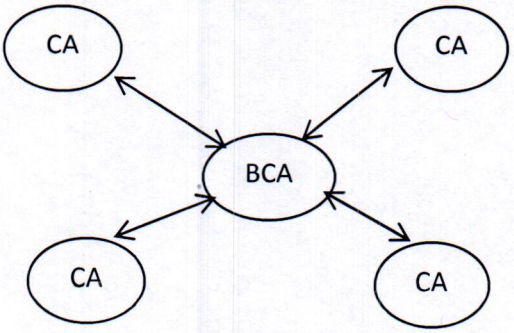


Figure 4.2: Hierarchical Trust Model

This model avoids interoperability problems, providing a well-defined strong structure for organized and centralized groups such as governments, the military, large multinational companies but on the other hand it could have some limitation for example security point of view about the root CA. Innovation and competition could be restricted by the technical policies imposed by CA [11].

Bridge CA

A Bridge CA (BCA) acts as a hub CA for a number of different PKIs. Each PKI joins to the BCA through their own Principal CA (PCA).The PCA may coincide with PKI trust anchors (for example, in a hierarchy the PCA is normally the trust anchor). Figure depicts four PCAs joined through a BCA. The PCAs would be in turn joined to their respective PKIs [9][14].



Using BCAs (in place o Figure 4.3: Bridge CA Model ırate PKIs) can decrease the total number of cross certificates required to join the PKIs. The BCA does not become a trust anchor for any of the PKIs as it is not directly trusted by any of the PKI entities. Rather trust is referenced from internal PKI trust anchors. The United States federal PKI (FPKI) project is attempting to join together multiple PKIs set up under separate federal agency programs using bridge CAs [5].

Cross-Certification (Mesh) Model

In this model, CAs are dealing as peers with each other and they are free to choose whether or not to trust each other. In case they trust on each other, the CAs issue cross certificate to each other. By this cross certification user can trace a certificate from an unknown CA back to a local trusted CA.

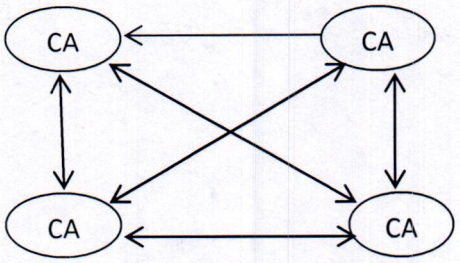


Figure 4.4: Cross-Certification Model

Interoperability is also challenging in mesh because it is not easy for a single pair of CAs to coordinate their policies and technical systems. Complexity of the system increases with the increase in the mesh system. Because of the cross certification, mesh is not an ideal approach for multinational PKI because of the unfamiliarity of CAs. In case where two or more related CAs are interoperating with each other. For example, two government departments with their own CAs might find it simple to cross certify each other for a particular tax application because their policies and technical specifications were already closely aligned [11].

Objective 2

Establishing interoperability via CPS (Certificate Practice Statement) and CP (Certificate Policy)

Certificate Policy

A Certificate Policy (CP) is a named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. It may be

used by a relying party to help in deciding whether the binding of the public key to the identified subscriber is sufficiently trustworthy for a particular use [20].

CPs includes the requirements for authenticating identity to the Certificate Authority in order to obtain a certificate, the requirements for securing the PKI, and how the keys are generated and stored. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business- to-business transactions for the trading of goods or services within a given price range.

The Certificate Policy (CP) defines certificate policies to facilitate interoperability among subscribers and relying parties for e-commerce and e-governance in India. The CP and Certifying Authorities (CAs) are governed by the Controller of Certifying Authorities (CCA). Secure e-commerce and e-governance in India is governed by the Information Technology (IT) Act 2000. In support of the IT Act of 2000 [17], the Government of India has developed and implemented the India Public Key Infrastructure (India PKI) [20].

Certification Practices Statement

A Certification Practices Statement (CPS) is a statement of the practices that a Certification Authority employs to govern issuing, managing, revoking, renewing and/or re-keying certificates in accordance with a specific Certificate Policy. The CPS establishes the proofing requirements for identifying the private key owner that must be satisfied before creating a certificate. There is a wide range of options for how robust (and resource intensive) this proof must be. The Certification Authority employs these procedures when issuing certificates, the clarification of parties' legal rights and obligations. CPSs may also be used to define the specific requirements of entities within the PKI performing other trusted roles. CPSs are generally reviewed for compliance with their associated Certificate Policy documents.

Objective -3

Establishing Efficient Techniques for Certificate Path Calculation and Validation

(a) Analysis of certificate policies to verify trust.
(b) Certificate path discovery and validation: interoperability for certification path validation is necessary to verify the evaluation of the difference between policies in the trust models

5. Proposed Approach

We have proposed a approach for handling inter-domain interoperability issues. This approach includes Cross-Certification and Bridge CA. This work as follows:-

1. Creation of Trust model
2. When a company wants to do communication with another, it first of all checks its certificate and certification authority.
3. If both are having certificate issued by the same CA, no issues and they can trust each other and make transactions. If no, then certificate mapping is done. In this approach we just try to make certificate policy automatic, at present it is being done manually [23].
4. If domains are different, issues arise, now we use one trusted third party (Authentication Server) who is responsible for checking and validating the certificate of each company.
5. Certificates are stored in Archive or Database for future reference.
6. RFC 2527 and RFC 3280 standards are followed.

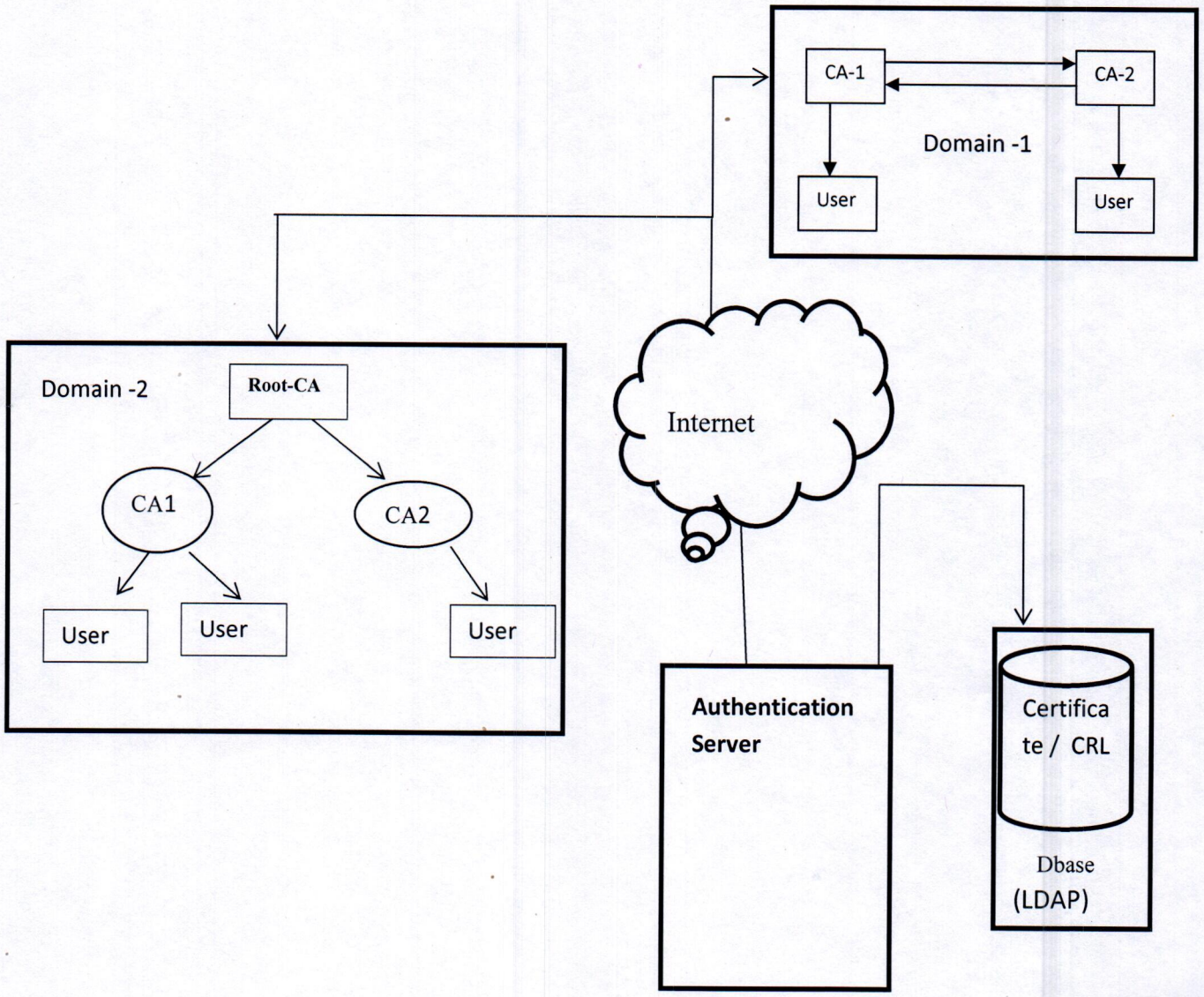


Figure 5.1 : Proposed Approach

6. Research Methodology

The proposed system will work as follows:-

1. Creation of Trust Model

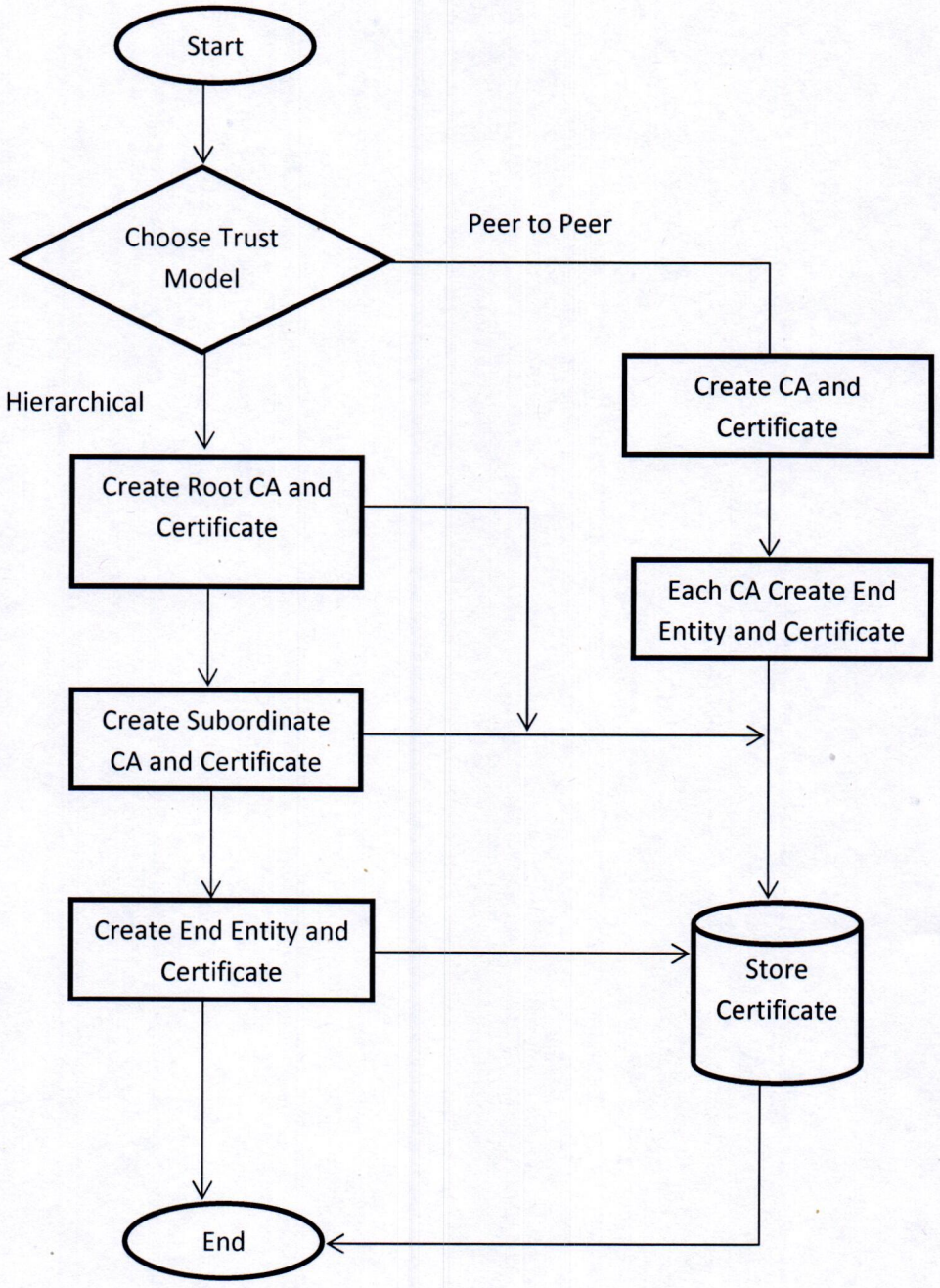


Figure 6.1 : Creation of trust model

2. Certificate Matching and Validation Algorithm

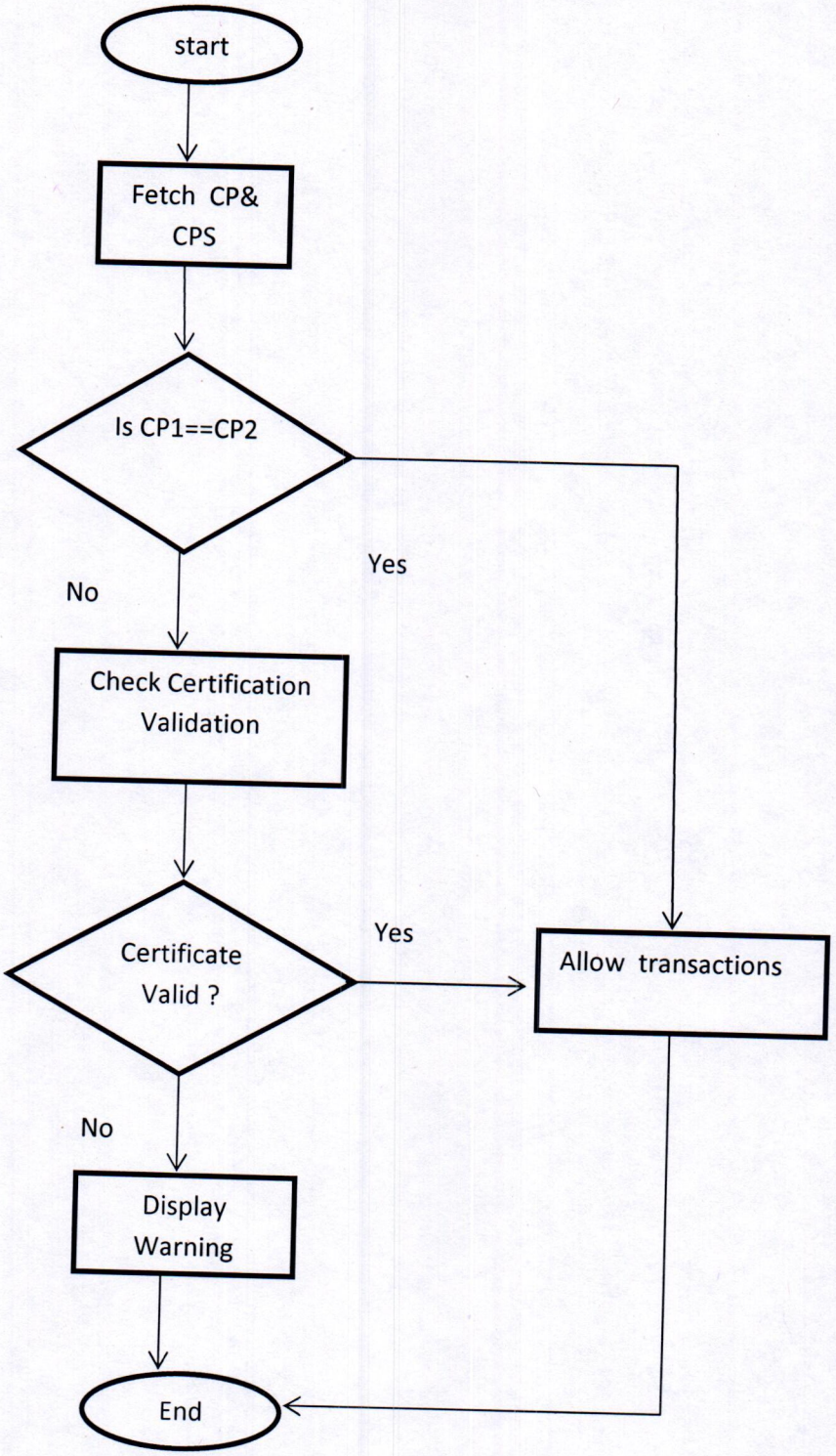


Figure 6.2 : Workflow of Matching of Certificate

7. Time Plan:

	Semester- I	Semester -II	Remarks
1st Year	Course work-1 (French & Research Methodology)	Course-work-2 (French & Public Key Infrastructure)	Completed successfully
2nd year	Study of Current State of PKI Implementations in the Real World. The first phase of the study entailed research on the current state of PKI Implementations and applications in the real world. To achieve entity authentication, the public key of each entity must be authentic and all the entities in the network should be able to validate its authenticity.	Development of a Scenario to Represent the Identified PKI Application.	State of the art in security and privacy in e-commerce.
3rd year	Continue with PKI certificate policy and certificate practice statement implementation.	Analyze against organizational goals (e.g., business cost and benefits) to determine the optimum PKI configuration.	Testing of the PKI

8. Hardware & Software Requirements:-

- Windows
- Java /OpenSSL
- PKI simulator

Conclusion

The security industry is moving to PKI and certificates for safe internet transactions. PKI is currently the only technology that provides the required level of data integrity and protection to support electronic commerce.
At the end of the research we would be able to design a system in which there is no inter-domain interoperability issue and provide hassle free secure communication among the end entities. Using PKI it also allows us to perform some tasks as:-

- Digitally signing files such as documents and applications.
- Securing e-mail from unintended viewers.
- Enabling secure connections between computers, even if they are connected over the public Internet or through a wireless network.
- Enhancing user authentication.

List of Publications

1. "Solution to PKI Inter- Domain Interoperability Issue", International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012 , ISSN 2229-5518. ((**Impact factor 1.4**)).
2. "Security issues in public key Infrastructure", Yamuna Journal of Technology and Business Research (ISSN:2250-3072).
3. "Threats & Security Issues in Ad hoc network: A Survey Report", International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-6, January 2013, pg. 138-143, Bhopal, ISSN: 2231-2307, indexed by –DOAJ,Google Scholar, getCITED, Yahoo India, .docstock, citeSeerx. **(Impact factor 1.0).**
4. "Trust Models in PKI", International Journal of Information & Computation Technology", Volume 3. Issue 6, March 2013, pp-502-506, Delhi, ISSN 0974-2239.

References

[1] PC Magazine Encyclopedia, www.pcmag.com, Accessed on 25th April, 2009.

[2] Diffie, Whitfield, and Martin Hellman. "New directions in cryptography."*Information Theory, IEEE Transactions on* 22.6 (1976): 644-654.

[3] Mazaher, Shahrzade, and Per Røe."A survey of state of the art in public key infrastructure." *Norwegian Computing Central report nr.995, 2003. URL: http://publications. nr. no/PKI_report. pdf* (2003).

[4] Jarupunphol, P. & Mitchell C. "PKI Implementation Issues in B2B E-Commerce." In U.E. Gattiker (Ed.), EICAR Conference Best Paper Proceedings(ISBN: 87-987271-2-5) 14 pages. Copenhagen: EICAR, 2003

[5] Adams, Carlisle, and Steve Lloyd. "*Understanding the Public-Key Infrastructure: Concepts, Standards and Deployment Considerations*." Sams Publishing, ISBN 1-57870-166-X , 1999.

[6] Kazerooni, A., M. Adlband, and O. Mahdiyar. "Application of public key infrastructure in E-business." *Proceedings of Recent Researches in Applied Informatics & Remote Sensing, 7th WSEAS International Conference on Applied Computer Science,* ISBN: 978-1-61804-039-8, ACM Digital library, 2011.

[7] Esfahaan University of Technology- "Introduction of Public Key Infrastructure (PKI) and X.509 Standard."In Persian.

[8] Lloyd, Steve, David Fillingham, Richard Lampard, Steve Orlowski, and John Weigelt. "CA-CA Interoperability."In *PKI Forum*, vol. 24. 2001.

[9] Ølnes, Jon. "PKI interoperability by an independent, trusted validation authority."In *5th Annual PKI R&D Workshop*Norway, pp. 4-6.2006 IEEE.

[10] Lloyd, Steven, et al. "PKI Interoperability Framework." *PKI Forum, http://www. pkiforum. org*. 2001.

[11] Guo, Zheng, TohruOkuyama, and Marion R. Finley. "A new trust model for PKI interoperability."In *Autonomic and Autonomous Systems and International Conference on Networking and Services, 2005.ICAS-ICNS 2005. Joint International Conference on*, pp. 37-37. IEEE, 2005.

[12] Zheng, Liping, and Yujuan Zhao. "Research on managing private key of PKI users."In *Mechatronic Science, Electric Engineering and Computer (MEC), 2011 International Conference on*, pp. 2411-2414, 978-1-61284-722-1/11/$26.00 ©2011 IEEE.

[13] Umair Ali. "Application of Public Key Infrastructure in E-Business."HochschuleFurtwangen University, Germany 2012.

[14] Chris Connolly, Peter van Dijk, Francis Vierboom and Stephen Wilson."PKI Interoperability Models."Galexia February 2005.

[15] Tai, Gwo-Chin, and Chung-Ming Ou. "The development of PKI interoperability in Taiwan."*Security Technology, 2003.Proceedings.IEEE 37th Annual 2003 International Carnahan Conference on*.IEEE, 2003.

[16] Vatră, Nicu□or. "Interoperability of Digital Signatures in Public Administration."*World of Computer Science and Information Technology Journal(WCSIT) ISSN: 2221-0741 Vol. 1, No. 6, 264-268, 2011.*

[17] PalashSarkar. "Public Key Infrastructure in India: Status and Issues." Applied Statistics Unit Indian Statistical Institute, Kolkata India, 2012.

[18] LeinHarn and JianRen."Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications", *Senior Member, IEEE,* IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 10, NO.7, JULY 2011, 1536-1276/11$25.00© 2011 IEEE.

[19] Fugkeaw, Somchart, PiyawitManpanpanich, and SekponJuntapremjitt. "AmTRUE: Authentication Management and Trusted Role-based Authorization in Multi-Application and Multi-User Environment." In *Emerging Security Information, Systems, and Technologies, 2007.SecureWare 2007. The International Conference on*, pp. 216-221. IEEE, 2007.

[20] X.509 Certificate Policy for India PKI, Controller of Certifying Authorities Department of Information Technology Ministry of Communications and Information Technology, 2010.

[21] Pala, Massimiliano, and Sean W. Smith. "Finding the PKI needles in the Internet haystack." *Journal of Computer Security* 18, no. 3 (2010): 397-420.

[22] Lioy, Antonio, Marius Marian, Natalia Moltchanova, and Massimiliano Pala. "PKI past, present and future." *International Journal of Information Security* 5, no. 1 (2006): 18-29 Springer.

[23] Muniyal, Balachandra, K. V. Prema, and MamathaBalachandra. "Comparison of Certificate Policies for Merging Public Key Infrastructures during Merger and Acquisition of Companies." *arXiv preprint arXiv:1210.2934* (2012).